

# How Can NSTIC & OIX Help Prevent Account Hijacking & ACH Fraud?

Bob Pinheiro

Robert Pinheiro Consulting LLC

[bob@bobpinheiro.com](mailto:bob@bobpinheiro.com)

# Introduction

- These are some preliminary ideas that describe how the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the Open Identity Exchange (OIX) can enable one pathway to strong cryptographic authentication for online banking and ACH payments.
- Please contact the author with any comments or suggestions.

# Background

## Problem

- Account hijacking
  - fraudulent access to online financial accounts
- ACH fraud
  - fraudulent payments / money transfers from banking accounts

## Root Causes

- Overreliance on passwords, “cookies”, and challenge questions
- MITM / MITB attacks on one-time passwords
- Weak or no authentication of transactions
- No authentication of online ACH payments based on use of bank routing number and account number

# FFIEC Authentication Guidance

- FFIEC Supplement to “Authentication in an Internet Banking Environment”, June 2011, recommends multifactor authentication for business customers.
- FFIEC Supplement acknowledges that
  - one-time passwords are subject to man-in-the-middle and man-in-the-browser attacks.
  - answers to challenge questions are easily discoverable.
- Although FFIEC recommends layered security for online banking, strong authentication methods resistant to these attacks should be deployed for business banking customers.

# Potential Solutions

- A. Smartcards containing client-side certificates for stronger authentication of authorized users and transactions:
- While no authentication method is foolproof, strong authentication based on client-side certificates is among the most secure of current alternatives.
  - Certificate doesn't have to include personal information, but just needs to be bound to an existing customer account by an authorized user.
  - Authentication just verifies (at some assurance level) that the person accessing the account controls the private key associated with the certificate initially bound to the account.

# Potential Solutions

## B. Trusted Platform Modules

- TPMs are components of many business-class laptop and desktop computers.
- TPMs allow generation of asymmetric (ie, public and private) cryptographic keys.
- These keys essentially provide a way to securely identify a particular computer.
- This provides a way to limit access to online accounts from specific computing devices.

# Why Don't We Have This Now?

- Distribution and management of certificates and keys is difficult and costly.
- Other “strong” authentication methods (challenge questions, one-time passwords) perceived as being more convenient, or “good enough”.
- Lack of support for client-side certificates and TPMs by online banking systems.

# Smartcards & TPMs

- Many individuals already have USB smartcards, or computers with TPMs, for access to their business networks and resources, or encryption of data:
  - numerous vendors (Ironkey, Gemalto, SafeNet, Verisign PIP, Vasco, etc) provide client x.509 certificates on these smartcards
  - many PC vendors (Dell, Lenovo, Gateway, etc) deploy TPMs on their business-class PCs
- Can these same certificates and TPMs be linked to the user's online business or consumer banking accounts for stronger authentication?

# Smartcards & TPMs

- If so, banks could provide strong authentication to a subset of their online banking customers without having to issue their own strong authentication credentials.
- Banks would need a way to determine whether authentication based on a non-bank-issued credential could be trusted.

# Smartcards & TPMs

- Although the subset of online banking customers already having client-side certificates on smartcards is small, if USB smartcards containing certificates can be made affordable for consumers, such devices could serve as a path to strong consumer authentication for banking, healthcare, government, etc.
- Consumer-class PCs as well as smartphones may eventually also contain TPMs for strong device authentication.

# How Can NSTIC & OIX Help?

- NSTIC and Open Identity Exchange (OIX) can support the development and listing of a Trust Framework (TF).
- The Trust Framework would specify policies, standards, and other rules that enable a bank to trust a certificate and smartcard it did not issue.
  - Perhaps based (in part) on the PIV-I (Personal Identity Verification – Interoperable) standards that enable the US gov't to trust certificates and smartcards it did not issue.

# How Can NSTIC & OIX Help?

- Once a TF is specified and deployed, individuals with trusted client-side certificates/smartcards should be allowed to link these certificates to their existing online financial accounts.
  - It's the bank's responsibility to initially ensure that the private key associated with a client certificate linked to an existing account is controlled by an authorized account holder.
  - These certificates wouldn't need to include personal identity information, so no worries about ID proofing.
  - Longer term, TFs could include identity proofing criteria, so trusted certificates could be used for enrollment in new high value financial services.

# How Can NSTIC & OIX Help?

- A Trust Framework can also specify the policies, rules, and standards that must be satisfied in order for a bank to trust that a device on which a TPM is deployed, and which the TPM has generated the appropriate keys, is authorized to access an online account.

# How Can NSTIC & OIX Help?

- Since NSTIC is voluntary, online banking systems should continue to provide other authentication methods for customers who do not choose to use these credentials.
  - But banks could offer incentives to those who do.
- Once an account is linked to a particular certificate/smartcard/TPM, anyone seeking access to the account must demonstrate control of the appropriate private key.
- To thwart social engineering, need strong procedures to allow account access if the private key is “lost”.

# Potential Assurance Issues

- Trust framework needs to define “high assurance” in terms of strength of the authentication technology and other attributes w/o necessarily being tied to someone’s actual identity.
- The assurance level associated with using the private key for authentication of an authorized user or device may depend on deployment options:
  - Higher assurance if private key is deployed on a Trusted Platform Module or removable smartcard
  - Lower assurance if private key is deployed directly on computer hard drive

# Other Challenges

- Vendors of online banking applications need to be “on board” by incorporating functionality to allow banking customers that already have client-side certificates or TPMs to link them to their accounts.
  - May need push from some big banks
- As mobile banking becomes more popular, it will be necessary to ensure that a customer’s certificate or TPM on a smartphone, in addition to one on a USB smartcard, can both be linked to the same customer account for strong authentication.

# Potential Next Steps

- Define the stakeholders
  - i.e., a few big banks and/or banking consortia, smart card vendors and/or consortia, online banking app vendors, fraud prevention groups
- Gather stakeholders and explore feasibility of working with Open Identity Exchange to create a Trust Framework for enabling banks to trust client certificates / smartcards / TPMs that banking customers already possess.
  - Would there be funding from interested stakeholders available to pursue this?
- Work with
  - online banking app vendors to incorporate necessary functionality into online banking apps.
  - NSTIC Program Office to keep abreast of related activities

# Conclusion

- The ability of banks to use cryptographic authentication can be enhanced if online banking apps could trust and accept certificates / smartcards / TPMs already in possession of customers.
- The use of USB smartcards to house client-side certificates provides a pathway to eventual adoption by consumers, since USB ports are ubiquitous on laptop and desktop computers.
- Strong online banking authentication based on client-side certificates or TPMs needs to work for customers who access their accounts from PCs as well smartphones.